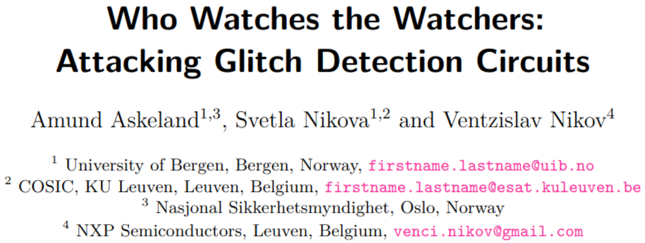
Attacking Glitch Detection Circuits

Amund Askeland

UNIVERSITY OF BERGEN

Attacking Glitch Detection Circuits



Who Watches the Watchers: Attacking Glitch Detection Circuits

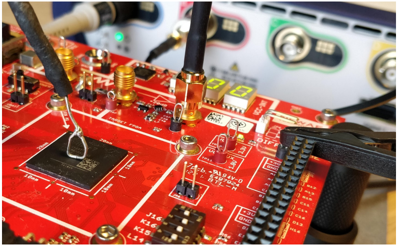
Amund Askeland[1,3], Svetla Nikova[1,2] and Ventzislav Nikov[4]

[1] University of Bergen, Bergen, Norway, firstname.lastname@uib.no
[2] COSIC, KU Leuven, Leuven, Belgium, firstname.lastname@esat.kuleuven.be
[3] Nasjonal Sikkerhetsmyndighet, Oslo, Norway
[4] NXP Semiconductors, Leuven, Belgium, venci.nikov@gmail.com

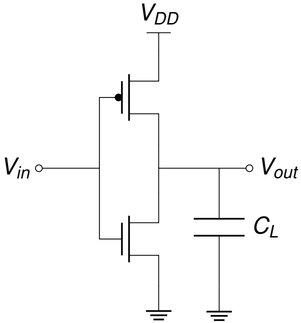
- This talk is based on [ANN23]

Fault Injection Attacks

- Provoke faulty computations in hardware
  - Some faults are exploitable
  - e.g faulty ciphertexts, incorrect branching
- Common methods are voltage and clock glitching
- Cause timing-violations in the target system



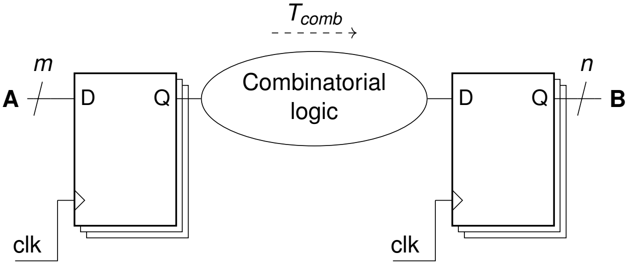
Timing in Hardware



Propagation Delay Due to Load Capacitance

$$t_{PLH} = \frac{C_L V_{DD}}{k_P (V_{DD} - V_{TP})^2}$$

Timing in Hardware

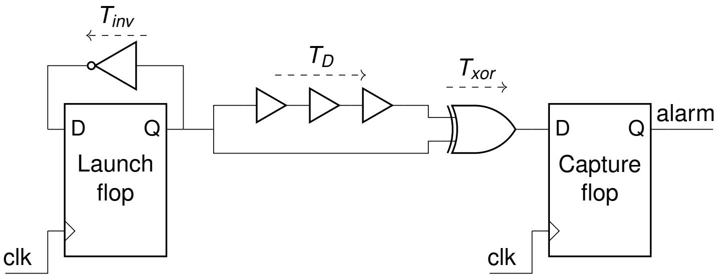


Timing Requirement for Synchronous Circuits

$$T_{clk} > T_{clk2Q} + T_{comb} + T_{setup}$$

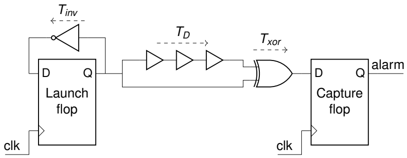
Glitch Detection Circuits

- Detectors as countermeasures
- A popular family of detector designs is based on "Parallel Delay Lines"

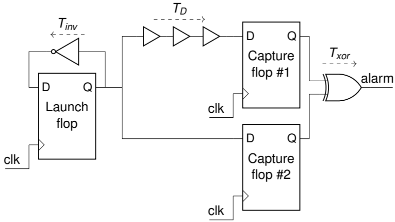


Glitch Detection Circuits

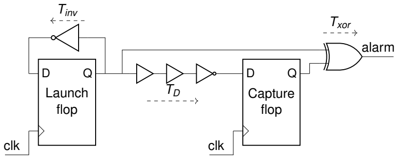
- Detectors as countermeasures
- A popular family of detector designs is based on "Parallel Delay Lines"



PDL-1



PDL-3



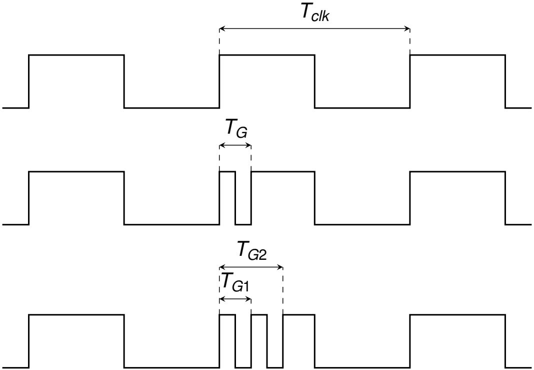
PDL-2

Attacking Glitch Detection Circuits

- The detectors work and can detect FIA
- Hard to prove a detector design
- Are there situations where these detectors can fail?

Clock Glitching

- One or more glitches added to the clock signal
- We use T_G to refer to the time of extra *rising* edges



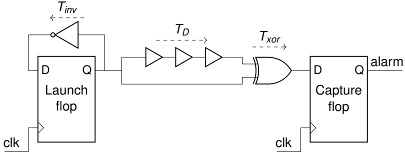
Experimental Setup

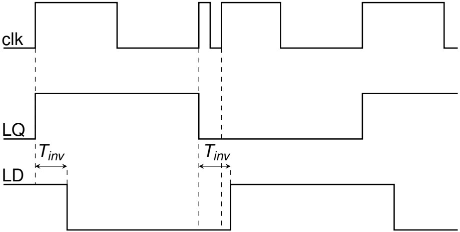
- Detectors and AES implemented on an FPGA
- Glitchy clock signal generated internally

Fault Alarm	No	Yes
Low	Negative	False Negative
High	False Positive	Positive

Attack 1

- Targets feedback inverter
- $T_G < T_{inv}$
- Applicable to PDL-1 and PDL-2

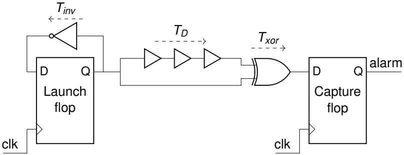


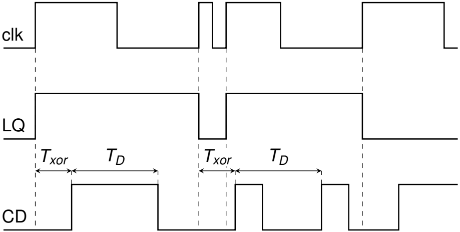


Attack 1 timing diagram

Attack 2

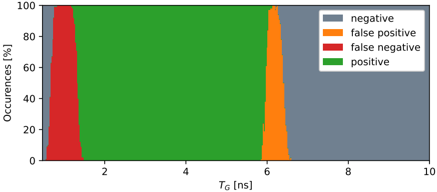
- Between inverter and xor
- $T_{inv} + T_{setup} < T_G < T_{xor}$
- Applicable to PDL-1



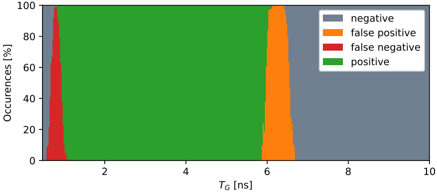


Attack 2 timing diagram

Results Attack 1 & 2

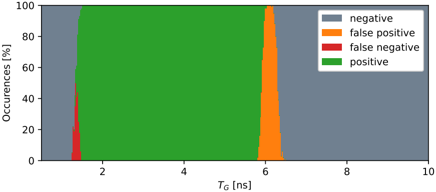


PDL-1

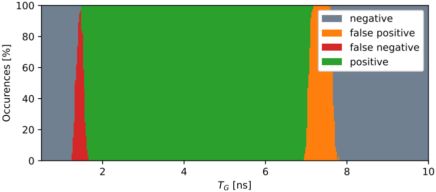


PDL-2

Results Using External Glitch Generator



PDL-1. $V_{INT} = 1\,\text{V}$



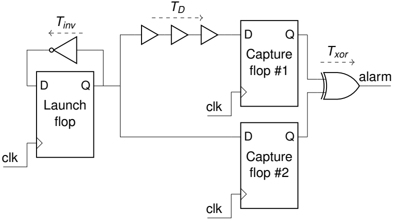
PDL-1. $V_{INT} = 0.93\,\text{V}$

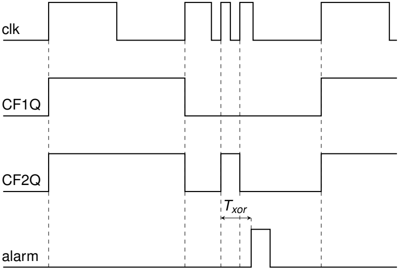
Double Glitch Attacks

- The single glitch attacks have strict requirements on T_G timing
- Using multiple glitches we have more options

Attack 3

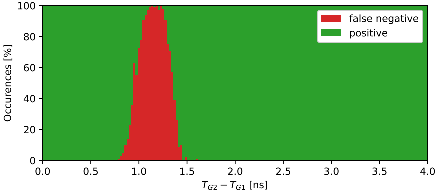
- Targets output xor
- $T_{G1} < T_D$ and
  $T_{G2} - T_{G1} < T_{xor}$
- Applicable to PDL-2 and PDL-3



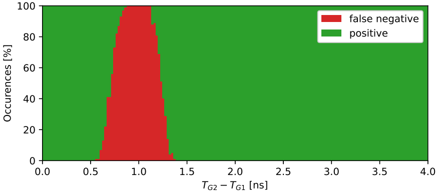


Attack 3 timing diagram

Results Attack 3



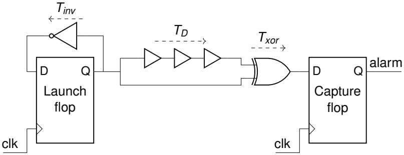
PDL-2

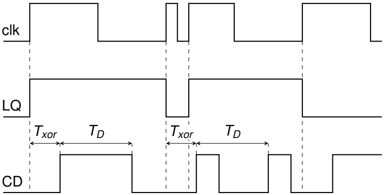


PDL-3

Attack 4

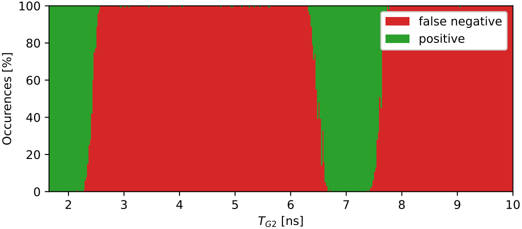
- Extension of attack 2
- $T_{inv} + T_{setup} < T_{G1} < T_{xor}$ and $T_{G1} + T_{xor} < T_{G2} < T_{xor} + T_D$
- Applicable to PDL-1





Attack 2 timing diagram

Results Attack 4



Conclusion

- Glitch detectors can fail
- There are countermeasures
- Room for improvement

References I

Amund Askeland, Svetla Nikova, and Ventzislav Nikov.
Who watches the watchers: Attacking glitch detection circuits.
Cryptology ePrint Archive, Paper 2023/1647, 2023.
https://eprint.iacr.org/2023/1647.

Questions?